International Journal of Computer and Engineering Optimization (IJCEO)
Volume 02, Issue 03, May – June (2024)

RESEARCH ARTICLE

CROW SEARCH OPTIMIZED DNA ENCRYPTION FOR SECURE MEDICAL DATA TRANSMISSION

Hari Krishna Kalidindi[1, *]

[1] Assistant Professor, Department of Computer Science and Engineering, SRKR Engineering College(A), Bhimavaram, W.G.Dt, India, 534204.

[*]*Corresponding e-mail: krishnavarma.kalidindi@gmail.com*

Abstract – Smart healthcare has become more and more popular as information technology has developed. In the contemporary information era, smart healthcare makes healthcare more efficient, convenient, and customized by completely changing the traditional medical system. Even if there are many ways that these advancements improve people's lives, one of the main concerns is still the security of the vast data transmission. In order to solve this issue, a novel approach on Crow search optimized DNA encryption for SEcure medical data Transmission (CD-SET), for secure data transmission through unsecure channel is introduced in this paper. The proposed CD-SET model enhances the data transmission security by employing robust cryptographic techniques while transmitting through an unsecure channel. Initially medical image input is given to the encryption algorithm which combines DNA encryption and homomorphic encryption. The data will be first encrypted using DNA sequencing based on the sequence of the four chemical bases such as A, C, G, and T that comprise DNA. The DNA sequencing is given as input for HE Encryption process in which the key generation is performed using crow search algorithm. Then, the cloud stores the encrypted data so that it can be accessed. Python simulator is used to evaluate the proposed technique. The efficiency has been evaluated using encryption, decryption and execution time with the existing technique. The recommended technique can be implemented in 3% less time with the Dynamic DNA encryption system and Cryptosystem using SHA-512 algorithm and 7% less time with the Robust S-Box building method algorithm.

Keywords *– Homomorphic algorithm, crow search optimization, encryption, decryption, data transmission.*

1. INTRODUCTION

The evolution of artificial intelligence and the Internet of Things has profoundly altered how humans live [1]. The security of the huge data transmission remains a crucial problem even if there are numerous instances in which these advances enhance life better. To address this problem, powerful cryptographic algorithms were designed and implemented [2]. Application attacks, however, are thought to pose serious threats to the present techniques while having an effect on the security of the system [3]. The ability of the aforementioned encryption methods to prevent misunderstanding is ensured by the Substitution Box (S-box), a built-in non-linear component in all of these algorithms [4]. Even if the data transport is made more complex by the S-boxes in AES and DES, they are unable to send large amounts of picture data and are vulnerable to assaults Compared to other popular encryption approaches, Chaotic encryption techniques might be more resilient to attacks. Neural network systems were used to create a high-security data protection methodology [5].

In terms of defending against side-channel assaults, the AES block encryption method exceeds the mathematically generated conventional S-boxes. With the assistance of 2DM-CPML, researchers generated a significant number of S boxes using a random S-box design process based on chaos. The idea of using chaos-based cryptography to provide effective encryption was initially put out [6]. By using modified block encryption methods and substitution permutation network designs, researchers advocated chaotic behaviour on information security [7, 8]. Several researchers opted for an edge computing architecture based on the Internet of Things for healthcare applications and employed chaotic systems to build incredibly complex crypto-analysis even after using S-boxes [16,17].

One of the applications of Internet of Things is healthcare is heavily reliant on the security of the channel. Therefore, sophisticated encryption techniques are required to protect patient privacy and data integrity. To counter the different security breaches caused by the Internet of Things, the healthcare sector's security protocols and practices need to be enhanced. In order to create more complex and incredibly arbitrary bits suitable for securely transmitting health data over IoT networks, the study seeks to inquire through this problem. A novel approach on Crow searches optimized DNA encryption for SEcure medical data Transmission (CD-SET), for secure data transmission through unsecure channel is introduced in this paper. The key goals of the paper are as follows.

- The proposed CD-SET model enhances the data transmission security by employing robust cryptographic techniques while transmitting through an unsecure channel.
- Initially medical image input is given to the encryption algorithm which combines DNA encryption and homomorphic encryption. The data will be first encrypted using DNA sequencing based on the sequence of the four chemical bases such as A, C, G, and T that comprise DNA.
- The DNA sequencing is given as input for HE Encryption process in which the key generation is performed using crow search algorithm. Then, the cloud stores the encrypted data so that it can be accessed.
- When another user accesses the data, after verification the image is decrypted and original image is transmitted to the verified user.

The remaining portion of the study is structured as follows: The literature review is represented in section 2. Section 3 provides a detailed representation of the proposed CD-SET technique. The experimental results are shown in Section 4, and Section 5 represents the conclusion and future work.

2. LITERATURE REVIEW

In 2020, Chen, Y. et al. [11] has explained another popular encryption method named as Hua's method. Pixel adaptive diffusion, key distribution, high-speed scrambling, and random data insertion make up the method. The permuted pixels have been dispersed using Modular Arithmetic (MA) and Bitwise XOR (BX). The encryption method utilizing BX is known as MIE-BX, and the method using MA is known as MIE-MA. Hua et al. have developed a pixel adaptive diffusion-based high- speed scrambling medical picture encryption technique.

In 2022, Akkasaligar, P.T. et al. [12] has recommended a novel multilevel cryptosystem using SHA- 512, heterogeneous hyper chaotic maps and DNA cryptography. The transmission of medical pictures via telecommunication was a feature of telemedicine and e-health systems. Medical photos can be altered or have noise added by hackers. It was exceedingly unlikely that the exact condition can be identified from the manipulated medical photos. Thus, it demonstrates that the suggested technique performs and was more efficient than the already used methods

In 2020, Akkasaligar, P. T. et al. [13] has suggested a high-level security for a digital medical picture using dual hyperchaotic map and DNA cryptography approaches Modern methods like telemedicine, smart health, and e-health have been used in the medical industry. The remote center has used the sent digital medical pictures for diagnosis. Therefore, ensuring the security and secrecy of the medical picture was a critical concern. The size of the digital medical pictures has been quite enormous, which takes additional computing time.

In 2022, El-Shafai, W. et al. [14] has presented research to deliver a more effective algorithm that satisfies key security needs including authentication, secrecy, and integrity while maintaining high resilience to a wide range of security threats. This hybrid optical-based system has been presented for the safe transmission of colour or grayscale medical pictures, even though insecure channels. The colour components of the plaintext medical picture have been compressed to create the compressed image components at the first security step using the Discrete Wavelet Transform (DWT)-based compressive sensing algorithm.

In 2022, El-Shafai, W. et al. [15] has recommended a reliable method based on a 3D chaotic map dependent cryptosystem for the encryption of medical images for the safe IoMT and cloud services. A 3D chaotic map has been the foundation of the suggested encryption technique. The XOR procedure, 3D chaos production, column and row rotation, have been among these operations. The recommended cryptosystem has been evaluated using a variety of medical photos with various features.

In 2022 Liu, H. et al. [16] has suggested an approach to create a robust S-Box building method that has been cryptographically keyed and relies on a non-degenerate 3D Improved Quadratic Map (3D-IQM). A 3D-IQM has been first built, and dynamics study showed that it has better unpredictability in phase space and was ergodic. In order to further increase the encryption's intensity, three arbitrary substitution-depth sequences have been constructed and used to randomly replace each pixel with an S-Box. The algorithm's security and efficacy were confirmed by experimental statistics and security analysis.

In 2023 Das, S. and Sanyal, M. K. [17] have devised a study based on dynamic DNA-based colour medical picture encryption system and a 3D unified chaotic system. The original image's pixels were first bit-level circularly rotated in the horizontal, diagonal and vertical directions. Following that, the locations of the DNA bases have been changed in various ways, resulting in severe DNA base shifting. The results of many tests have been incredibly positive and demonstrate effective encryption execution on all types of pictures.

3. PROPOSED MODEL

In this section, a novel approach on Crow searches optimized DNA encryption for SEcure medical data Transmission (CD-SET), for secure data transmission through unsecure channel is introduced in this paper. The proposed CD-SET model enhances the data transmission security by employing robust cryptographic techniques while transmitting through an unsecure channel. Initially medical image input is given to the encryption algorithm which combines DNA encryption and homomorphic encryption. The data will be first encrypted using DNA sequencing based on the sequence of the four chemical bases such as A, C, G, and T that comprise DNA. The DNA sequencing is given as input for HE Encryption process in which the key generation is performed using crow search algorithm. Then, the cloud stores the encrypted data so that it can be accessed. When another user accesses the data, after verification the image is

decrypted and original image is transmitted to the verified user. Figure 1 represents the proposed model.

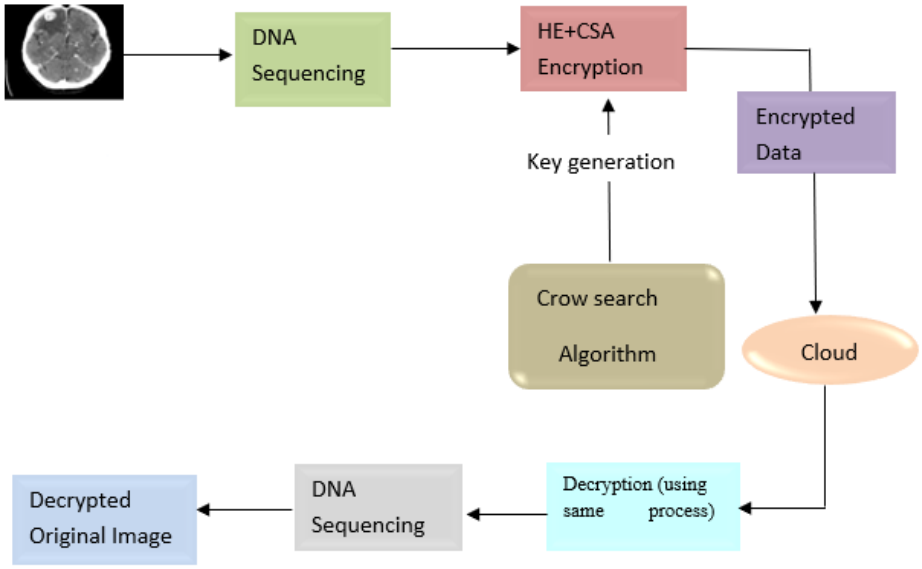

Figure 1. Architecture of Proposed Method

3.1. Key generation using CSO

The key for the CD-SET is generated using Crow Search Optimization (CSO) which ensures security. The crow search algorithm relies on the behaviour and knowledge of crows.

Phase 1: Key initialization and encoding

Initially, a random key value is chosen, and that key is then sent as input to the solution encoding procedure.

Phase 2: Fitness Estimation

The fitness of each solution is calculated after the solution generation process. Throughput is considered a measure of fitness. Fitness is determined by using equation (1)

$$S = Maximum\ (F) \tag{1}$$

Phase 3: updating CSO

In this step, the CSO updates the solution after evaluating the fitness value. This updating process involves two cases.

Scenario 1: Let us consider crow m and crow n as possessors. If the possessor crow m travels to the food source S_m^n in this scenario, crow n will follow the possessor crow m and reach the food source S_m^n. Crow n updates its position based on the food supply. Eq. (2) gives the Updating function.

$$W_h^{n+1} = w_h^n + l_h \times w_h^n \times (y_h^n - w_h^n) \tag{2}$$

where, l_h denotes the arbitrary number in the range [0, 1], w_h^nrepresents the fight length of the crow h at b iteration

Scenario 2: If the possessed crow m realizes that the crow n is following, the situation will alter. In this case, equation (3) is used to update the location of crow.

$$w_h^{n+1} = \begin{cases} if\ l_h \geq Z_h^w\ update\ poistion \\ else \quad update\ to\ random\ position \end{cases} \tag{3}$$

where Z_h^w represents the probability. The crow's position is converted into a binary form using a sigmoid transformation $H\ n$. Its formation is illustrated by the following equation:

$$F\ n\ (w_h^{n+1}) = \frac{1}{1+\exp -w_h^n} \tag{4}$$

The new position w_k^{n+1} of the crow is determined after the sigmoid transformation

$$w_h^{n+1} = \begin{cases} 1\ if\ G_{S\,n} < H\ n\ (f_h^{n+1}) \\ o, otherwise \end{cases} \tag{5}$$

where $T_{H\,n}$ denotes the number generated randomly between the range of [0, 1].

Phase 4: Termination Process

The iteration will stop once the best fitness function is obtained. BA represents the attained optimal solution

3.2. DNA sequencing

After being transformed into binary values, the medical image is next mapped to DNA sequences.

Table 1. Binary values for DNA bases

DNA	BINARY VALUES
A	00
G	01
C	10
T	11

The four nitrogenous bases of DNA are thymine (T), adenine (A), guanine (G), and cytosine (C). The use of the four nucleotides in the sequence is the most significant aspect of the DNA-based data masking process. A DNA sequence can be made up of any combination of these nucleotides. When DNA is sequenced, the order of bases can be determined, and they may be represented by a single letter in

plain sequence format. Binary values for DNA bases are given in Table. 1.

In the above table, the binary values for the DNA bases have been given, on this basis the medical image will be transformed.

3.3. DNA Homomorphic Encryption

Homomorphic encryption allows users to compute encrypted data without decrypting it first. Using homomorphic encryption, the same mathematical operations on encrypted or decrypted data get the same results since the structure of the data in a homomorphic encryption system remains the same. Homomorphic encryption relies mostly on addition and multiplication, as opposed to Boolean functions, and requires very few interactions. The four operations of this mechanism are key generation, encryption, evaluation, and decryption, which can optionally decrypt the assessment algorithm details. In the proposed method, the homomorphic algorithm is used for encryption and crow search optimization algorithm is used for key generation which reduces the privacy challenges raised from the homomorphic encryption.

Homomorphic encryption, as a public key cryptosystem, has the added benefit of authenticating the image or data. Each step in the decryption process contributes to the decryption of the assessment algorithm specifics, including key generation, encryption, evaluation, and decryption. The outcome is the same as if the operation had been carried out on the initial messages. Programmers use a number of variables to determine the encryption plot depending on the operation they are performing.

3.4. Decryption

A decryption process can restore unencrypted data to its original, unencrypted state. Decryption involves gathering and converting the jumbled data into text and graphics that can be understood by both readers and computers. Decryption can be done either manually or automatically. A combination of keys or passwords can also be used.

$$Decrypted\ image\ = \frac{Z(D^{\omega}\ mod\ Key_{opt}^{2})}{Z(Z^{\omega}\ mod\ key\ _{opt}^{2})}\ mod\ key \qquad (6)$$

In the above equation, A represents cipher text, Z represents public key and ω represents Euler's totient.

4. RESULT AND DISCUSSION

The result section explains the comparison analysis on encryption, decryption and execution time between the existing methods and proposed technique. Encryption, decryption and execution time comparative analysis were made between Dynamic DNA encryption system, Cryptosystem using SHA-512 and Robust S-Box building method and (CD-SET) proposed technique across ten images. Shown in Table 2 and 3.

Table 2. Comparative analysis of the encryption time

Images	Dynamic DNA-encryption system	Cryptosystem using SHA-512	robust S-Box building method	CD-SET (Proposed)
1	5	7.2	9.5	10
2	5.3	7.5	9.2	10.5
3	5.2	7.1	8.5	9.2
4	5.8	8	8.3	9.7
5	4.5	6.5	8.2	9.8
6	4.9	6.8	8.2	9.9
7	5.2	7.2	8.5	10
8	5.3	6.9	9	10.4
9	4.2	7	9.2	11
10	4	6.1	9.5	11.3

Encryption is done to securely store the input medical data, which is shown in figure 2. The medical images are encrypted and stored in the cloud and can be accessed only by the user. An unauthorized user cannot able to access the images. For decryption, the same method is repeated and the reconstructed original image is obtained. First, the medical images will be converted into binary format and then into a DNA sequence, which will be given as input. Comparative evaluation of the encryption and decryption times is shown in Tables 2,3.

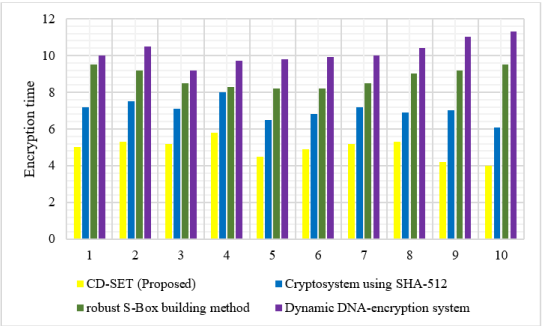

Figure 2. Comparative analysis of the encryption time

Table 3. Comparative analysis of the decryption time

Images	Dynamic DNA-encryption system	Cryptosystem using SHA-512	robust S-Box building method	CD-SET (Proposed)
1	7	9.2	11.5	11.8
2	6.2	9.3	11.3	11.9
3	6.3	9.5	10.8	11.5
4	6	9.8	10.9	10.7
5	6.8	9.7	10	11.2
6	6.5	9.5	10.5	10.7
7	6	9.4	10.9	11.5
8	6.2	8.8	10.8	11.4
9	6.5	8.5	10.6	11.5
10	6.8	8.9	10.5	11.3

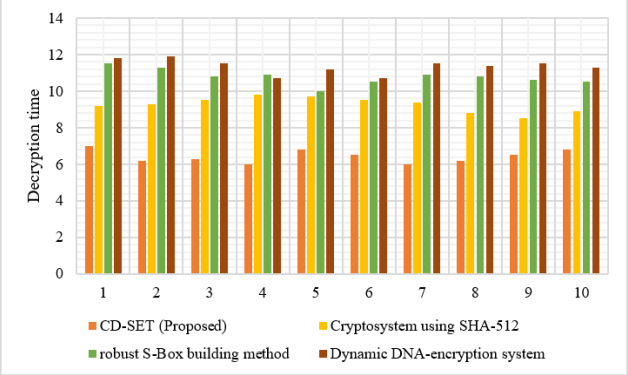

Figure 3. Comparative analysis of the decryption time

Fig. 3 depicts a comparison of the proposed method's decryption times to known methods such as Dynamic DNA encryption system, Cryptosystem using SHA-512 and Robust S-Box building method. Fig 3 shows the encryption time of the recommended approach. Cloud authentication is a means of encrypting or transforming data as it is transported to cloud storage. Cloud Service provider companies encode data and transmit the encryption keys to the user. For decrypting the data, these keys are required. For the decryption time, it is advised that the Cryptosystem using SHA-512 algorithm be reduced by 2% and the Robust S-Box building method algorithm by 34%.

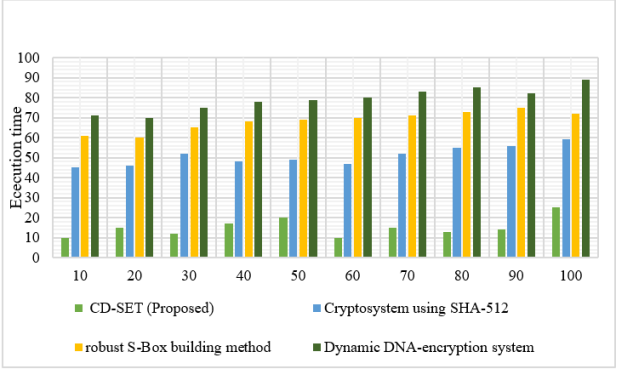

Figure 4. Comparative analysis of the execution time

The proposed system and the existing approach are compared in Fig. 4 at the time of implementation. The new method's implementation time is quicker than the current one. The recommended technique can be implemented in 3% less time with the Dynamic DNA encryption system and Cryptosystem using SHA-512 algorithm and 7% less time with the Robust S-Box building method algorithm.

5. CONCLUSION

In this paper, a novel approach on Crow search optimized DNA encryption for SEcure medical data Transmission (CD-SET), for secure data transmission through unsecure channel is introduced. The proposed CD-SET model enhances the data transmission security by employing robust cryptographic techniques while transmitting through an unsecure channel. Initially medical image input is given to the encryption algorithm which combines DNA encryption and homomorphic encryption. The data will be first encrypted using DNA sequencing and then given as input for HE Encryption process in which the key generation is performed using crow search algorithm. The image processing method is evaluated using a Python simulator. Encryption, decryption and execution time comparative analysis were made between Dynamic DNA encryption system, Cryptosystem using SHA-512 and Robust S-Box building method and (CD-SET) proposed technique across ten images. The recommended technique can be implemented in 3% less time with the Dynamic DNA encryption system and Cryptosystem using SHA-512 algorithm and 7% less time with the Robust S-Box building method algorithm. In Future, various optimization algorithm can be deployed for secure image transmission through network and intrusion detection technique for identifying malicious attacks.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest.

FUNDING STATEMENT

Authors did not receive any funding.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] D. Selvathi, and R. Chandralekha, "Fetal biometric based abnormality detection during prenatal development using deep learning techniques", *Multidimensional Systems and Signal Processing,* pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools and Applications,* vol. 80, pp. 21165-21202, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] H. M. Waseem, S. S. Jamal, I. Hussain, and M. Khan, "A novel hybrid secure confidentiality mechanism for medical environment based on Kramer's spin principle", *International Journal of Theoretical Physics,* vol. 60, pp. 314-330, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] D. Kumar, V. Sudha, and R. Ranjithkumar, "A one-round medical image encryption algorithm based on a combined chaotic key generator*," Medical & Biological Engineering & Computing,* vol. 61, no. 1, pp. 205-227, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] W. El-Shafai, I. Almomani, A. Ara, and A. Alkhayer, "An optical-based encryption and authentication algorithm for color and grayscale medical images", *Multimedia Tools and Applications,* pp. 1-36, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Das, A. K. Das, and N. Kar, "An Improved Chaos based medical image encryption using DNA encoding techniques", in Advances in Computational Intelligence, Security and Internet of Things: Second International Conference, ICCISIoT 2019, Agartala, India, December 13–14, 2019, Proceedings 2, 2020, pp. 207-220: Springer. [CrossRef] [Google Scholar] [Publisher Link]

[7] V. Raj, S. Janakiraman, and R. Amirtharajan, "Reconfigurable color medical image encryptor using hardware accelerated Chao (S)-box triplets", *Journal of Real-Time Image Processing,* vol. 20, no. 2, pp. 27, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] B. Ahuja, R. Doriya, S. Salunke, M. F. Hashmi, and A. Gupta, "Advanced 5D logistic and DNA encoding for medical images", *The Imaging Science Journal,* pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] D. R. Ramji, C. A. Palagan, A. Nithya, A. Appathurai, and E. J. Alex, "Soft computing based color image demosaicing for medical Image processing", *Multimedia Tools and Applications,* vol. 79, no. 15, pp. 10047-10063, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] S. Zafar, N. Iftekhar, A. Yadav, A. Ahilan, S. N., Kumar, and A. Jeyam, "An IoT method for telemedicine: Lossless medical image compression using local adaptive blocks", *IEEE Sensors Journal,* vol. 22, no. 15, 15345-15352, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion", *Signal Processing,* vol. 167, p. 107286, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] P. T. Akkasaligar, S. Biradar, and S. Biradar, "Multilevel security for medical image using heterogeneous chaotic map and deoxyribonucleic acid sequence operations", *Concurrency and Computation: Practice and Experience,* vol. 34, no. 24, pp. e7222, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] P. T. Akkasaligar, and Sumangala Biradar, "Selective medical image encryption using DNA cryptography*", Information Security Journal: A Global Perspective,* vol. no. 2, 91-101, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] W. El-Shafai, I. Almomani, A. Ara, and A. Alkhayer, "An optical-based encryption and authentication algorithm for color and grayscale medical images", *Multimedia Tools and Applications,* pp. 1-36, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie, "Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services", *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-28, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] H. Liu, J. Liu, and C. Ma, "Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption", *Multimedia Tools and Applications,* pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] S. Das and M. K. Sanyal, "Dynamic key generator based colour medical image protection algorithm using 3D unified chaotic system and dynamic DNA coding", *International Journal of Information Technology,* vol. 15, no. 2, pp. 1015-1033, 2023. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

Hari Krishna Kalidindi Presently working As Assistant Professor in Department of Computer Science &Engineering from SRKR Engineering college since 2017.

Arrived: 23.05.2024
Accepted: 24.06.2024